

Published and Copyright (c) 1999 - 2005  
All Rights Reserved

Atari Online News, Etc.  
A-ONE Online Magazine  
Dana P. Jacobson, Publisher/Managing Editor  
Joseph Mirando, Managing Editor  
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor  
Joe Mirando -- "People Are Talking"  
Michael Burkley -- "Unabashed Atariophile"  
Albert Dayes -- "CC: Classic Chips"  
Rob Mahlert -- Web site  
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,  
log on to our website at: [www.atarinews.org](http://www.atarinews.org)  
and click on "Subscriptions".  
OR subscribe to A-ONE by sending a message to: [dpj@atarinews.org](mailto:dpj@atarinews.org)  
and your address will be added to the distribution list.  
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE  
Please make sure that you include the same address that you used to  
subscribe from.

To download A-ONE, set your browser bookmarks to one of the  
following sites:

<http://people.delphiforums.com/dpj/a-one.htm>  
<http://www.icwhen.com/aone/>  
<http://almag.atari.org>  
Now available:  
<http://www.atarinews.org>

Visit the Atari Advantage Forum on Delphi!  
<http://forums.delphiforums.com/atari/>

=~==~==

~ U.S. Recruits Hackers! ~ ID Theft Ring Found! ~ Firefox Update!  
~ Blog Visitors Growing! ~ Spam Assets Seized! ~ MS Wins Spam Case!

-\* Columbus Atari Swapmeet Near \*-  
-\* U.S. Passes the Buck on ID Theft! \*-  
-\* Internet Scammers Keep Working in Nigeria! \*-

~~~~~

->From the Editor's Keyboard "Saying it like it is!"  
"~~~~~"

I'm not usually a name-dropper, but the weather this week reminds me of that famous line in "The Wizard of OZ," lamented by that Wicked Witch of the East as she encountered a bucket of water: "I'm Melting, I'm melting..." It has been sweltering here in the northeast this past week. The heat and humidity was simply unbearable. I don't have much on my mind to speak about this week, and this weather is not helping with brain energy! So, let's move right along and get to this week's issue.

Until next time...

~~~~~

Zview BETA 6

Hi all,

Zview BETA 6 is available.

I'm grateful to every beta-testers and would especially like to thank Sascha Uhlig for his great work on the documentation ( which is better than the software itself :) and for the desktop icon.

Well, the most important news features are:

- PDF support
- Godpaint read and write
- Animated Gif
- Zoom function

Due to a G++ bug, only the FPU version are available this time :/

ZcodecLib and Zweather are also updated to match with the new codecs format.

Ciao,  
Zorro

--

Webpage: <http://zorro.arcadia-crew.com>  
 Blog: <http://zorro-arcadia.blogspot.com>

GFA-Basic Editor v1.20 Released

The most important new feature in this release is the direct support for RUN! Software's new RUN!Only interpreter. The instant satisfaction you got from hitting the 'Run' button is back.

Related links if you wish to download the RUN!Only interpreter.  
<http://www.run-software.de/>  
<http://www.run-software.de/runonly.htm>

Many other new features and corrections, too many to list here. Please see the documentation for both programs for details. See the URL in my signature to download the updated editor.

Enjoy.

```
--
FreeMiNT      http://sparemint.atariforge.net/sparemint/ [Free your mind...]
Atari Team    http://setiathome.berkeley.edu/team_display.php?teamid=30472
L. Pursell    http://www.bright.net/~gfabasic/ [AtarIRC, GFA-Basic, Hades060]
```

$$= \sim = \sim = \sim =$$

```
->A-ONE User Group Notes!   - Meetings, Shows, and Info!  
    " " " " " " " " " " " " " " " " " " " " " "
```

## Atari Swapmeet To Be September 10

Here are details for the annual swapmeet to be held next month by the Columbus Atari club:

DATE: Saturday, September 10, 2005.  
TIMES: 9 am to 3 pm.  
ADMISSION: \$4. (For vendors, including table: \$6.)  
PLACE: Oakland Park Community Building, 980 Lenore Avenue,  
Columbus, Ohio.  
MORE INFO AT: <http://www.angelfire.com/oh4/acec/acec.html>  
CONTACT: R. Wayne Arenz (rarenz at columbus dot rr dot com)

$$\equiv \sim \equiv \sim \equiv \sim \equiv$$

PEOPLE ARE TALKING

compiled by Joe Mirando  
joe@atarinews.org

Hidi ho friends and neighbors. Another week has come and gone, and Mother Nature is still feeling the need to supply the northeast with plenty of heat and humidity. Well, that's kind of to be expected this time of the year, so I'm not really complaining.

For those of you who read my column last week, I did get to watch one of my other favorite movies... FORBIDDEN PLANET.

If you've never seen the movie, think about renting it sometime. There's lots of good stuff throughout the movie to get you thinking, or to get you running to the computer to check on whether or not that's... "really that guy" or if Robby is really the same robot that appeared in <fill in the blank>.

I've been a Sci-Fi fan for as long as I can remember. The reason I got interested in computers in the first place was Star Trek's Mr. Spock. Even back then, I realized that I'd never get to go zooming out among the stars, but computers might... just might, mind you... become a reality in my lifetime.

Ten years later, there they were, and I got bitten by the bug early on. No, they weren't the thinking/speaking machines of Star Trek and various other science fiction movies or series, but they were the ember that just might burst into a flame if technology moved the way that experts estimated it would.

I can remember my Computer Science professor telling us that music on a computer would never be possible because digital waveforms didn't lend themselves to natural sounding sounds. A brief diagram of a sinewave-like analog wave next to the blocky, stair-step looking 'digital' sound wave briefly convinced me that he was correct.

Of course, the state-of-the-art machine at the time was an Apple ][ with a 9" monochrome monitor and cassette tape drive. Not many of us back then envisioned multi-gigahertz, multi-gigabyte broadband-enabled computers, but I guess we should have.

Now, as we near the limits of what you can etch into a piece of silicon, I wonder what new twist or turn of technology will surface to keep our computers going faster and faster. Gallium Arsenide? X-Ray etching? Optical circuits? Who knows, but whatever it is, it'll make for some interesting machines. I guess all we can do is wait and see.... Unless, of course, you have the knowledge and funding to CREATE the future. In that case, just drop me an email and let me know what to invest my money in, huh? <grin>

Well, let's get to the news, hints, tips and info available from the UseNet.

From the comp.sys.atari.st NewsGroup  
=====

Phil Graham asks about his MegaSTE's ailing hard drive:

"I own a 4mb Mega STe running 2.06 TOS. However my hard drive (a Seagate ST32155N 2.1gb) connected to the ASCI port fails to boot now. The drive was formatted with HDDriver v8.0.

The drive does 'whir' up on power up but does not boot. The HDDriver software finds the ASCI device but no Hard Drive.

Firstly.. is the hard drive beyond saving?

Secondly is there anyway of recovering the data using a PC?"

Coda tells Phil:

"You didn't say which SCSI interface you're using. Maybe its this which is dead and not the drive? Have you any other SCSI devices you can put on the bus to see if they work/recognize?"

Dr. Uwe Seimet, author of HD Driver, asks Phil:

"It finds the device, but no drive? Can you elaborate? Do you mean that something like "ACSI 0.0" is reported, but the drive name is missing?

Do I understand it correctly that this drive worked before, and even though you did not change anything regarding your hardware setup it does not work anymore? If this is the case it sounds bad. But maybe it's just a broken cable. If the device is recognized, but the name (only a few bytes) cannot be transferred a broken cable can easily cause that.

I doubt that you'll be able to recover data using a PC. Actually, my experience is that it is even more difficult to recover anything with a PC because the more low level access is required the less you can do it with a PC. If a device does not report its name anymore there is something fundamentally wrong.

But nevertheless it's worth a try: A PC running Linux should be able to access the TOS-compatible partitions of this drive if they can be accessed at all.

Ensure that under no circumstance anything is written to this drive. If data are garbled while being transferred trying to write something will make things even worse."

Phil answers:

"I'm using the ACSI interface which is inside my Mega STE.

When I click on Device check it says "Bus 0: Atari ACSI". But if I try Format it doesn't list any devices.

The drive worked until yesterday. I then installed a new Power Supply Unit (Atari's own) into my MSTe. As I mentioned, the drive does power up ok."

Uwe tells Phil:

"[Since it worked recently] it simply must have something to do with changing the power supply. Either the new power supply does not work correctly or something was broken when installing it."

Phil replies:

"For the past 6 hrs I thought i'd lost everything!!

Anyway I found the problem.... a jumper had fallen off my HD (parity disabled) whilst I was installing my PSU... dohh!"

'Phantom' takes to opportunity to post this:

"While on the subject of Mega STE Internal Hard Drive, I've a few questions.

I have a Mega STE TOS 2.06, 4megs High Density Floppy Drive and Internal Hard Drive using the Factory hard drive hardware.

Actually, due to lack of space at the moment, I've not used it that much and is in storage. But I plan on setting it up as I move stuff around.

My questions are these:

Will the internal Factory Hard drive hardware support more than one SCSI hard drive, if I can make room inside the case? Using HD Driver?

If so, what starting version would be ok to run it like this?

(Reason I ask, my original new version of HD Driver seems to be damaged) (I've never used it or installed it before) Going to check it on another system to make sure that it isn't my floppy drive.

And, can I run 2 scsi drives on the Factory hardware and also use a few more drives like another SCSI, CDRW/CDROM using a ICD Link II or a Link 97? (I have both devices.) on the DMA port?

Since I have a Vortex 386SX board installed, I'd like to use it with DOS on a small SCSI on the Factory hardware. And have another SCSI drive just for TOS stuff. Possibly choosing which drive to boot from on start up if possible. If not, it isn't a big problem. I've the manual to guide me on setup.

I want to experiment with Terminal Programs on the 386SX such as Net-Tamer and a few others, and since the MegaSTE has 2-3 modem ports it will be fun for me to see what I can get running on those ports. I have a CD here called (So Much Modem Madness 2) with over 6000 programs, mostly in DOS stuff. I've had it for along time and would like to see what I can find that will work.

However, I have wondered if HD Driver does increase the size of the DOS Boot partition, and DOS partitions with PC hardware emulators like the Vortex 386SX and the FalconSpeed 286 board. As the boot partitions are a bit small. However, with FalconSpeed you can access fairly large partitions even Tos ones if memory serves me correctly. But I've not much experience with the 386SX Vortex yet.

Another question that's probably be asked a lot, but I can't remember the answer.

On A MegaSTE with Factory High Density Floppy Drive, If I connect a second floppy drive, whether it is a DS/DD or a 1.44 High Density Drive. Will the MegaSTE setup for the right drive, or do I need to change a setting in either software or inside with a switch?

Can I just plug in any drive such as a 5 1/4 Floppy 720K IB Drive, DS/DD or High Density and the MegaSTE will know what's connected? (I hope this is the way it works).

I know HD Driver is Good. However I have the original English MegaSTE system Disk and Atari Advanced Hard Drive software for the MegaSTE.

I have heard that the internal hard drive hardware can be touchy. So should I use the Atari hard drive software that's was for the MegaSTE hard drive or go with a version of HD Driver?

Another question, Is the MegaSTE limited to 19200 Baud or can one use HSMODEM7 to get better speed out of all the modem/serial ports?

And if HSMODEM will work, is this only program available to gain those extra speeds?

It has been awhile since I setup a good Atari from scratch. So I need a little refresher on these things.

Any help is most appreciated.

BTW, Any one have a very clean working MEGA STE keyboard for trade? My MSTE looks like new, but the keyboard is a bit yellowed. Contact me if ya do."

Uwe tells Phantom:

"No, the internal host adaptor won't handle more than one drive. You need another host adapter for this.

Registered users of HD Driver of course get a free replacement by email if their binaries are damaged.

You can use up to 7 devices with the Link97, but you have to ensure that the cables are short if you actually want to connect so many.

The HDDRIVER manual contains information on how to boot from different partitions.

With HDDRIVER the TOS (!) boot partition may be as big as any other partition, but HDDRIVER cannot lift any restrictions your PC emulation may have.

There are search machines for newsgroup searches. Actually a lot of the questions asked here have been asked and answered many times in the past.

The internal drive is a hard disk drive like any other. There's nothing special with it."

David Moeser tells posts this about the Columbus Atari Club's annual swapmeet:

" DATE: Saturday, September 10, 2005.  
TIMES: 9 am to 3 pm.  
ADMISSION: \$4. (For vendors, including table: \$6.)  
PLACE: Oakland Park Community Building,  
980 Lenore Avenue, Columbus, Ohio.  
  
MORE INFO AT: <http://www.angelfire.com/oh4/acec/acec.html>  
CONTACT: R. Wayne Arenz (rarenz at columbus dot rr dot com)"

Someone anonymous (let's call them 'Tia', because that's how they signed their posts... TIA. <G>) asks for help with a confused hard drive:

"I have no idea how but my main drive (C) has become write protected.  
Does anyone know how I can remove this???"

Edward Baiz tells Tia simply:

"If you have HDDdriver you can remove it."

Tia replies:

"I have HDDDriver 8+ but that only protects the root and boot sectors and it won't even do that because it's saying that drive C is write protected. Can't find any other setting to fix the problem. I'm on an STe with TOS 2.06 and 4mb ram."

Steve Sweet tells Tia:

I'd have thought there'd be a driver /ancillary application setting to fix that. Boot using a floppy based driver and look for switches."

Mark Duckworth adds:

"I think this can happen due to disk errors. It depends if the disk has the S.M.A.R.T stuff or not. Someone else might be able to confirm it. I know if Linux (I know, a bit higher level) detects errors it immediately remounts the filesystem read-only. What's to stop disk manufacturers from doing this low level on critical errors, in order to protect the integrity of the data."

Uwe Seimet interjects:

"I have never heard of drives that write protect themselves in case of an error. That does not mean that such drives do not exist, but I would expect to have heard of them."

Phantom asks Tia:

"Have you tried running Diamond Edge or some other good Hard Drive



utility program that will look for corrupted files and fragmentation?

If not, try and see if how the Data on Drive C looks. The drive may need De-Fragmented or errors corrected.

Also, not sure if this has anything to do with your problem. But the Cartridge Port's default letter is Drive C. And I would think it would be write protected since its the cartridge port.

Are you sure your Hard Drive C is booting up online?"

Derryck Croker corrects Phantom:

"If I remember correctly, that would be a lower-case "c" for the cartridge port, by the way."

Jean-Luc Ceccoli asks about transfer speeds on his CT60:

"On my FalCT60 100/20 MHz, with an IDE HD capable of 100 MB/s transfer rate and a CD burner capable of 7.2 MB/s, with HD-Driver 8.13, the actual transfer rate is only of 2.5 MB/s, though the rate displayed during boot is 6.3 MB/s (CT60 utility rev. 1.03a from march 2005).

Is my Falcon faulty, or do they all behave the same way?"

Mark Duckworth tells Jean-Luc:

"I think mine does something similar to this. I tested real write operation with filesystem overhead and everything and it too was somewhere around 2.5MB/sec. Perhaps there's a bottleneck inside freemint or TOS? I'd love faster disk throughput. A real 15-20MB/sec would be a dream."

Stephane Perez adds:

"IMHO the bottleneck is called Videl. I have a 30 GB IDE disk (a Maxtor that was running in UDMA 66 mode in an old PC) and I made some tests on my FalconCT60 100/16 (no motherboard boost). It can reach 2.9 MB/s with Freemint when the Videl is switched off, it can easily be done with a program called Turbo Veille: you press on some keys simultaneously and the screen becomes black, giving to the 68060 (or 68030) all the machine time.

Before using Turbo Veille the transfer rate was only 2.5 MB/s. You can download this program here:

[http://www.geocities.com/SiliconValley/Vista/6443/t\\_veille.zip](http://www.geocities.com/SiliconValley/Vista/6443/t_veille.zip) "

'Peter' adds his own thoughts:

"While the Videl certainly slows things down, the biggest (smallest?) bottleneck is the 16 bit, 16/25Mhz bus. No way around that.

Have a look at the benchmarks (ST-RAM speeds) at the URL below.

[http://www.czuba-tech.com/CT60/english/benchs\\_eng.htm](http://www.czuba-tech.com/CT60/english/benchs_eng.htm)

"Tony Montana has a huge following. He's become a part of popular culture. His likeness is sold by street painters, Scarface posters are everywhere, people often list the movie as among their top 10 favorites and several rappers have said that he's an inspiration (for their music)," said game

producer Cam Weber.

The game starts where screenwriter Oliver Stone and director Brian De Palma's remake of the original 1932 film ends - Montana, a penniless Cuban refugee who became one of the most feared drug lords in the United States, greets assassins in his Miami mansion with a big gun and the now famous line "Say hello to my little friend."

But, instead of dying in a blaze of bullets, he escapes and returns several months later to kill again.

Pacino lends his likeness to the game, but not his voice. Another actor "who's a dead ringer for Pacino" assumed the role of Montana in the game, Weber said.

Other actors from the 1983 film, including Steven Bauer, who played Montana's sidekick Manny Ribera, Robert Loggia (played Frank Lopez) and Miriam Colon (as Mama Montana) return. The game is due out in mid-2006.

#### EA's Madden NFL 06 Hits Store Shelves

Electronic Arts announced that Madden NFL 06, the newest iteration of the EA SPORTS best-selling football franchise with the exclusive videogame license of the NFL and PLAYERS INC, is on store shelves today. Reflecting the focus on the passing game in the NFL, Madden NFL 06 has changed passing for the first time in ten years with the all-new QB Vision Control and QB Precision Placement and introduces the all new NFL Superstar mode, where you can live the life of an NFL Superstar.

Madden NFL 06 continues to be at the forefront of innovation and gameplay with all new features this year. Madden NFL 2005? since the launch has sold over six million copies, and was the #1 selling sports videogame of 2005 in North America. Madden NFL 06 has already started a fan frenzy with pre-sell reservations outpacing last year?s and numerous midnight store openings around the country to ensure all fans receive their copy as early as possible. Adding to early demand is the fourth annual EA SPORTS Madden Challenge, played exclusively this year on the Xbox video game system from Microsoft, kicks off August 27th in Las Vegas with a \$100,000 grand prize check for the Finals winner. Tournament runs on published dates in each city. For additional details and Tournament Official Rules see <http://www.maddenchallenge.com>.

For the first time in 10 years, the Madden NFL Football franchise has revolutionized its passing game, giving Madden NFL 06 the most groundbreaking and innovative offensive arsenal ever created. The new QB Vision Control lets you scan the field, look off defenders, and make perfect throws within your quarterback?s unique field of vision. QB Precision Placement lets you put the ball exactly where you want it. Plus, all new Truck Stick Control delivers the big hits on offense to break tackles, pancake defenders, and clear your path to the end zone.

NFL Superstar is an entirely new single-player mode allowing you to experience the life of an NFL player by earning one of more than 60 Personas ranging from MVP to Movie Star. Features include choosing your parents, hiring an agent, getting drafted into the NFL, visiting tattoo parlors, choosing different movie roles, and even getting the chance to play in the coveted EA SPORTS Madden Bowl.

Madden NFL 06 is the only video game to offer fantasy capabilities featuring EA SPORTS Fantasy Football integration for the first time. You are now able to check your fantasy scores, get trade notifications and earn trophies in Madden NFL 06. This year's game continues to have unprecedented depth and upgrades with more robust online features including sharing files via your EA Locker, allowing more online players to access these files with friends or backup those crucial files you don't want erased. It is essentially an online memory card that that you can make accessible to friends. Madden NFL 06 comes to the PSP on September 20 with a unique version of the game, allowing consumers to take the biggest sports franchise ever on the go with the PSP (PlayStation Portable) entertainment system.

In its 16th year and with more than 43 million copies sold, Madden NFL Football continues to stand out as the most popular football videogame franchise of all time with a combination of innovative new features and the most authentic football gameplay. Developed in Orlando, FL by EA Tiburon Madden NFL 06 is now on the PlayStation 2 computer entertainment system, the Xbox video game system from Microsoft, Nintendo GameCube, Nintendo DS, and Game Boy Advance. PC will be available August 17 and PSP launches on September 20. Madden NFL 06 is rated 'E' (Everyone) by the ESRB and has an MSRP of \$49.99 for the PlayStation 2 console, Xbox, Nintendo GameCube and PSP, \$39.99 for PC and Nintendo DS, \$29.99 for Game Boy Advance.

#### New Pay Service Creates Online Gaming Arena

GameSpot, one of the most popular Web sites for video game enthusiasts, has started a new subscription online service where hard-core gamers can battle each other in the most popular online computer games.

Dubbed a "premium gaming service," GameSpot Game Center will offer \$9.99-a-month subscriptions to gamers who will be able to play at the highest speed connections in online games such as Electronic Arts' "Battlefield 2." It will offer discussion groups, voice chat services and tournaments as well. GameSpot is owned by online portal CNet Networks.

The object is to create a cool gaming experience with fast game play and connections with like-minded gamers.

Services like this have failed in the past, but largely because they involved spending a lot of money on computer servers. GameSpot has found a way to reduce that expense by leasing them from a third party.

It remains to be seen if gamers will pay to play online games that they can play for free via the Internet. But GameCenter product manager Sam Parker says GameCenter removes a lot of the hassles from online gaming.

GameCenter will allow players to host their own online games. That means it will allow them to configure a Battlefield 2 game and customize it to their tastes so that as many as 64 players can fight it out without annoying hiccups in broadband service that slow down a game and make it all but impossible to play. About 11 games are available through GameCenter now.

GameCenter will be able to offer server hosting because it is leasing computing power from Super Computer International, an Atlanta Internet hosting company. GameCenter will be able to tap data centers on both the

East Coast and West Coast to provide plenty of high-speed service, or bandwidth, to gamers.

GameSpot already offers game-downloading services and extended news coverage of games for \$6.95 a month via a service called GameSpot Complete. Those subscribers can upgrade to the GameCenter subscriptions.

GameSpot has no plans to publish its own online games now. Rather, it plans to partner with game publishers who may not want to operate their own paid online-gaming services.

"We can become the distribution partner for the game publishers," said Henk Van Neikerk, vice president of paid services at GameSpot.

GameSpot competes with other game portals such as Ign.com, and it draws about 20 million gamers a month to its Web site.

#### Man Dies After 50 Hours of Computer Games

A South Korean man who played computer games for 50 hours almost non-stop died of heart failure minutes after finishing his mammoth session in an Internet cafe, authorities said on Tuesday.

The 28-year-old man, identified only by his family name Lee, had been playing online battle simulation games at the cybercafe in the southeastern city of Taegu, police said.

Lee had planted himself in front of a computer monitor to play online games on Aug. 3. He only left the spot over the next three days to go to the toilet and take brief naps on a makeshift bed, they said.

"We presume the cause of death was heart failure stemming from exhaustion," a Taegu provincial police official said by telephone.

Lee had recently quit his job to spend more time playing games, the daily JoongAng Ilbo reported after interviewing former work colleagues and staff at the Internet cafe.

After he failed to return home, Lee's mother asked his former colleagues to find him. When they reached the cafe, Lee said he would finish the game and then go home, the paper reported.

He died a few minutes later, it said.

South Korea, one of the most wired countries in the world, has a large and highly developed game industry.

=~::~~::~=

## Internet Scammers Keep Working in Nigeria

In Festac Town, an entire community of scammers overnights on the Internet. By day they flaunt their smart clothes and cars and hang around the Internet cafes, trading stories about successful cons and near misses, and hatching new plots.

Festac Town is where communication specialists operating underground sell foreign telephone lines over which a scammer can purport to be calling from any city in the world. Here lurk master forgers and purveyors of such software as "e-mail extractors," which can harvest e-mail addresses by the million. Now, however, a 3-year-old crackdown is yielding results, Nigerian authorities say.

Nuhu Ribadu, head of the Economic and Financial Crimes Commission, says cash and assets worth more than \$700 million were recovered from suspects between May 2003 and June 2004. More than 500 suspects have been arrested, more than 100 cases are before the courts and 500 others are under investigation, he said.

The agency won its first big court victory in May when Mike Amadi was sentenced to 16 years in prison for setting up a Web site that offered juicy but phoney procurement contracts. Amadi cheekily posed as Ribadu himself and used the agency's name. He was caught by an undercover agent posing as an Italian businessman.

This month the biggest international scam of all - though not one involving the Internet - ended in court convictions. Amaka Anajemba was sentenced to 2 1/2 years in prison and ordered to return \$25.5 million of the \$242 million she helped to steal from a Brazilian bank.

The trial of four co-defendants is to start in September.

Day in, day out, a strapping, amiable 24-year-old who calls himself Kele B. heads to an Internet cafe, hunkers down at a computer and casts his net upon the cyber-waters.

Blithely oblivious to signs on the walls and desks warning of the penalties for Internet fraud, he has sent out tens of thousands of e-mails telling recipients they have won about \$6.4 million in a bogus British government "Internet lottery."

"Congratulation! You Are Our Lucky Winner!" it says.

So far, Kele says, he has had only one response. But he claims it paid off handsomely. An American took the bait, he says, and coughed up "fees" and "taxes" of more than \$5,000, never to hear from Kele again.

Festac Town, a district of Lagos where the scammers ply their schemes, has become notorious for "419 scams," named for the section of the Nigerian penal code that outlaws them.

Why Nigeria? There are many theories. The nation of 130 million, Africa's most populous, is well educated, and English, the lingua franca of the scam industry, is the official language. Nigeria bursts with talent, from former NBA star Hakeem Olajuwon to Nobel literature laureate Wole Soyinka.

But with World Bank studies showing a quarter of urban college graduates are unemployed, crime offers tempting career opportunities - in drug dealing, immigrant-trafficking, oil-smuggling, and Internet fraud.

The scammers thrived during oil-rich Nigeria's 15 years of brutal and corrupt military rule, and democracy was restored only six years ago.

"We reached a point when law enforcement and regulatory agencies seemed nonexistent. But the stance of the present administration has started changing that," said Ribadu, the scam-busting chief.

President Olusegun Obasanjo is winning U.S. praise for his crackdown. Interpol, the FBI and other Western law enforcement agencies have stepped in to help, says police spokesman Emmanuel Ighodalo, and Nigerian police have received equipment and Western training in combating Internet crime and money-laundering.

Experts say Nigerian scams continue to flood e-mail systems, though many are being blocked by spam filters that get smarter and more aggressive. America Online Inc. Nicholas Graham says Nigerian messages lack the telltale signs of other spam - such as embedded Web links - but its filters are able to be alert to suspect mail coming from a specific range of Internet addresses.

Also, the scams have a limited shelf life.

In the con that Internet users are probably most familiar with, the e-mailer poses as a corrupt official looking for help in smuggling a fortune to a foreign bank account. E-mail or fax recipients are told that if they provide their banking and personal details and deposit certain sums of money, they'll get a cut of the loot.

But there are other scams, like the fake lotteries.

Kele B., who won't give his surname, says he couldn't find work after finishing high school in 2000 in the southeastern city of Owerri, so he drifted with friends to Lagos, where he tried his hand at boxing.

Then he discovered the Web.

Now he spends his mornings in Internet cafes on secondhand computers with aged screens, waiting "to see if my trap caught something," he says.

Elekwa, a chubby-faced 28-year-old who also keeps his surname to himself, shows up in Festac Town driving a Lexus and telling how he was jobless for two years despite having a diploma in computer science.

His break came four years ago when the chief of a fraud gang saw him solve what seemed like "a complex computer problem" at a business center in the southeastern city of Umuahia and lured him to Lagos.

He won't talk about his scams, only about their fruits: "Now I have three cars, I have two houses and I'm not looking for a job anymore."

## U.S. Passes the Buck on Identity Theft

One year ago, President George W. Bush signed into law the Identity Theft

Penalty Enhancement Act in response to the growing proliferation of Internet scams, such as phishing, pharming and other ploys aimed at stealing consumers' private information electronically. One year later, however, the evidence suggests that this new law has done nothing to reduce identity theft or fraud.

Rather, the number of publicly known identity theft cases has increased dramatically over the past year. Since January of 2005, there have been over 63 data-security breaches exposing nearly 50 million identities. And there will be more, according to industry insiders.

ChoicePoint, LexisNexis, Wells Fargo, Bank of America and CardSystems are just a few examples of recent security breaches that led to the loss of sensitive consumer information. Some security experts - albeit mostly in the software industry - believe that laws such as the Identity Theft Penalty Enhancement Act and the CAN-SPAM Act of 2003 have proven to be ineffective in the fight against Internet crime.

Instead, they say companies must take responsibility for implementing new protective technologies that address these vulnerabilities head on. Others argue that the federal government has to fix what does not yet work in its ID theft legislation.

The Identity Theft Penalty Enhancement Act (ITPEA) establishes penalties for identity theft committed in connection with the commission of a felony. From a legal standpoint, the new law merely updates existing penalties and brings identity theft into the electronic age. Perhaps its most stringent scare tactic is to prescribe a two-year jail term for anyone convicted of using somebody else's identity in connection with a felony. In essence, it doubled the incarceration penalty.

The law connects identity theft to violations of various sections of the Social Security Act and the false acquisition of others' Social Security and veterans' benefits. The law also makes it more difficult for judges to issue more lenient penalties.

Because some courts do not consider the totals from all counts for the purpose of imposing sentences, the change in the new law results in longer prison sentences by those courts. Also, the law prevents judges from placing any person convicted of such a violation on probation.

According to Marc Hubbard of the Texas law firm of Munsch Hardt Kopf & Harr, the ITPEA and the CAN-SPAM Act were primarily intended to make for easier prosecution and punishment of the perpetrators, once caught.

"But no law will deter all bad acts, and this one is not likely to have much deterrent effect, given that many of the perpetrators are outside the U.S.," Hubbard wrote in an e-mail exchange. "It may take prosecution of a number of cases before any deterrent effect within the U.S. kicks in."

R. "Doc" Vaidhyanathan, vice president of product marketing and corporate development for security firm Arcot Systems, does not see much impact coming from the new federal laws. He wants to see more effort made by government to make it easier for law enforcement officials to get convictions.

"From what we can see, things aren't changing a lot," said Vaidhyanathan. "On one hand we see an increase in the reporting of losses from ID scams. In reality, the higher numbers might just reflect better monitoring."



Kris Lovejoy, the CTO of Consul Risk Management, also does not see much good coming from the one-year-old federal law. It lacks both provisions for funding and the creation of standards to regulate what happens with electronic data.

"Statistics are not yet released from the Federal Trade Commission (FTC). But I have to assume the ID theft trend is increasing," said Lovejoy.

She sees part of the problem falling on the logistics of law enforcement. Because most offenders are prosecuted on the state levels, the new federal law has not yet had a chance to get results. To change that, Lovejoy wants to see the federal government get more proactive. "Both the federal government and private industry need to do more," she said.

Some in the computing industry think that the new federal legislation is reaping benefits even if it isn't curtailing identity theft. For instance, the law is prompting a greater awareness about identity-theft safety in consumers.

"It carries a sense of safety with it," said Terrence DeFranco, CEO of Edentify, a company that offers software products that screen databases for names that are at high risk for being incidences of identity fraud. "No one wants to deliberately place personal information at risk."

Still, DeFranco does not see much change coming from the year-old law. He believes that education and increased safety measures by consumers will make more of a difference in cutting down on identity theft than ITPEA will.

That legislation does not address the nature of today's data, said DeFranco. Information handling has changed over the last decade. Ten years ago, even the news media had trouble getting public records. Now, reporters and consumers can find everything they want to know about anybody on the Internet.

"Personal information gets into the public domain very quickly. We get nearly instant credit applications," DeFranco said about how easily consumers' personal information is shared.

According to Arco's President and CEO, Ram Varadarajan, the federal identity theft law is not effective because it only addresses one part of the problem and identity theft can take many forms.

Friendly theft, for instance, refers to theft by family and associates. For example, an ex-spouse or partner can use known information to execute financial transactions. The defrauded person is not likely to press charges in these cases, and increasing the penalty makes it even less likely that charges would be filed.

Lost data is another type of identity theft that is not always clear cut. For example, a list of credit card numbers, by itself, is not a big security risk. It is only when these numbers are combined with other personal information - like date of birth, home phone number and other such "permanent" information - that the loss becomes significant. The law does not penalize an organization that lost the data, only the fraudsters who use the data.

A final category, which some call malicious theft, is the only one targeted by the existing laws. Malicious theft pertains to phishers and fraudsters who circulate viruses and Trojan programs that are designed to extract

consumers' personal information and transmit it to the fraudster.

Critics of the federal legislation cite its largely unenforceable nature as the primary reason it will not work. The higher penalty is of little value, they say, if the identity thief cannot be caught. These malicious thefts often are committed by faceless criminals who are well hidden and distributed worldwide, said Varadarajan.

As such, there is no one single corporate entity that prosecutors can go after. Instead, prosecutors have to chase a trail of false-name fronts and sift through large volumes of data to track individuals who are involved in this kind of crime. The effort required to deliver the level of proof necessary for a conviction is large, burdensome and often beyond the ability of law enforcement teams working with limited budgets.

"In this light, those committing phishing, virus, Trojan and other forms of malicious attack programs operate knowing that there is a very low probability of being caught and even a lower probability of being found guilty," Varadarajan said. "As such, increasing the penalty in this context does not help. Laws should help increase the probability of being convicted in the first place."

Attorney Hubbard believes that legislators have to write laws that hold information handlers more accountable. Obviously, the law is not a substitute but is rather a complement to effective technical measures, caution and common sense by consumers, he said.

The next step, from a legal point of view, might be laws directed at increasing the liability of those who fail to implement available technical countermeasures. "Businesses very likely would strongly oppose any shifting responsibility to them," said Hubbard. "The mere possibility of such laws may, however, embolden them to make more radical changes in their payment systems."

What Hubbard alludes to is new federal-level laws patterned after California's mandatory disclosure and notification act. That law, one of the toughest in the nation, requires companies whose consumer data is stolen to notify consumers of the potential identity theft.

Consul Risk Management's Lovejoy wants to see things go even a bit further. She wants tougher state laws along with a hardened federal approach. "If we take the concept of ITPEA, which is too lenient anyway, and apply it on the state level, we may have some effect on those who commit identity thefts," said Lovejoy.

On the other hand, Edentify's DeFranco says the approach pushed by Lovejoy and others is vilifying the wrong people. He firmly believes that companies handling consumer data do not deliberately let their guard down to have consumer information stolen.

"The bad guy is the one doing the crime, not the company that has the information stolen," DeFranco said.

#### Students Charged With Computer Trespass

They're being called the Kutztown 13 - a group of high schoolers charged with felonies for bypassing security with school-issued laptops,

downloading forbidden Internet goodies and using monitoring software to spy on district administrators.

The students, their families and outraged supporters say authorities are overreacting, punishing the kids not for any heinous behavior - no malicious acts are alleged - but rather because they outsmarted the district's technology workers.

The Kutztown Area School District begs to differ. It says it reported the students to police only after detentions, suspensions and other punishments failed to deter them from breaking school rules governing computer usage.

In Pennsylvania alone, more than a dozen school districts have reported student misuse of computers to police, and in some cases students have been expelled, according to Jeffrey Tucker, a lawyer for the district.

The students "fully knew it was wrong and they kept doing it," Tucker said. "Parents thought we should reward them for being creative. We don't accept that."

A hearing is set for Aug. 24 in Berks County juvenile court, where the 13 have been charged with computer trespass, an offense state law defines as altering computer data, programs or software without permission.

The youths could face a wide range of sanctions, including juvenile detention, probation and community service.

As school districts across the nation struggle to keep networks secure from mischievous students who are often more adept at computers than their elders, technology professionals say the case offers multiple lessons.

School districts often don't secure their computer networks well and students need to be better taught right from wrong on such networks, said Internet expert Jean Armour Polly, author of "Net-mom's Internet Kids & Family Yellow Pages."

"The kids basically stumbled through an open rabbit hole and found Wonderland," Polly, a library technology administrator, said of the Kutztown 13.

The trouble began last fall after the district issued some 600 Apple iBook laptops to every student at the high school about 50 miles northwest of Philadelphia. The computers were loaded with a filtering program that limited Internet access. They also had software that let administrators see what students were viewing on their screens.

But those barriers proved easily surmountable: The administrative password that allowed students to reconfigure computers and obtain unrestricted Internet access was easy to obtain. A shortened version of the school's street address, the password was taped to the backs of the computers.

The password got passed around and students began downloading such forbidden programs as the popular iChat instant-messaging tool.

At least one student viewed pornography. Some students also turned off the remote monitoring function and turned the tables on their elders\_ using it to view administrators' own computer screens.

The administrative password on some laptops was subsequently changed but some students got hold of that one, too, and decrypted it with a

password-cracking program they found on the Internet.

"This does not surprise me at all," said Pradeep Khosla, dean of Carnegie Mellon University's engineering department and director of the school's cybersecurity program.

IT staff at schools are often poorly trained, making it easy for students with even modest computer skills to get around security, he said.

Fifteen-year-old John Shrawder, one of the Kutztown 13, complained that the charges don't fit the offense. He fears a felony conviction could hurt his college and job prospects.

"There are a lot of adults who go 10 miles over the speed limit or don't come to a complete stop at a stop sign. They know it's not right, but they expect a fine" not a felony offense, he said.

Shrawder's uncle, James Shrawder, has set up a Web site that tells the students' side of the story.

"As parents, we don't want our kid breaking in to the Defense Department or stealing credit card numbers," said the elder Shrawder, a businessman. "But downloading iChat and chatting with their friends? They are not hurting anybody. They're just curious."

The site, <http://www.cutusabreak.org>, has been visited tens of thousands of times and sells T-shirts and bumper stickers, including one that says: "Arrest me, I know the password!"

The district isn't backing down, however.

It points out that students and parents were required to sign a code of conduct and acceptable use policy, which contained warnings of legal action.

The 13 students charged violated that policy, said Kutztown Police Chief Theodore Cole, insisting the school district had exhausted all options short of expulsion before seeking the charges. Cole said, however, that there is no evidence the students attacked or disabled the school's computer network, altered grades or did anything else that could be deemed malicious.

An association of professional computer educators, The International Society for Technology in Education, believes in a less restrictive approach to computer usage. The more security barriers a district puts in place, the more students will be tempted to break them down, it believes.

"No matter how many ways you can think to protect something, the truth is that someone can hack their way around it," said Leslie Conery, the society's deputy CEO. "The gauntlet is thrown down if you have tighter control."

#### Spyware Researchers Discover ID Theft Ring

Spyware researchers picking apart one of the more notorious spyware programs have stumbled upon what appears to be a massive identity theft ring hijacking confidential data from millions of infected computers.

Sunbelt Software Inc., makers of the enterprise-grade CounterSpy spyware protection product, made the discovery during an audit of "CoolWebSearch," a program that routinely hijacks Web searchers, browser home pages and other Internet Explorer settings.

During the research, Sunbelt researcher Patrick Jordan deliberately installed the "CoolWebSearch application on a machine and immediately noticed that the infected system became a spam zombie that was placing callbacks to a remote server.

When Jordan visited the remote server, he was shocked to find that it was being used to distribute sensitive personal information from millions of PC users infected by the spyware application.

"We found the keylogger transcript files that are being uploaded to the servers. We're talking real spyware stuff-chat sessions, usernames, passwords, bank account information, full names, addresses," said Sunbelt president Alex Eckelberry.

[Read more here about the many faces of spyware.](#)

In an interview with Ziff Davis Internet News, Eckelberry said the sophistication of the operation suggests it's the work of a "massive identity theft ring" that used keystroke loggers to grab confidential information that could be used to create fake online identities.

"I'm not being dramatic. This is the most repulsive thing I've ever seen. It's very painful to see what's in these log files that are being uploaded in real time. We're seeing a lot of bank information and usernames and passwords to get in," Eckelberry said.

He said the log files included logins to one business bank account with more than \$350,000 and another small company in California with over \$11,000, readily accessible.

"There are lots of eBay account information and names and addresses of the people owning those accounts. Names, passwords, all matched up," Eckelberry added.

He said the server, which is hosted out of a data center in Texas, was effectively a "massive repository of stolen data" that was being replenished in real time.

"As the [log] file gets to a certain size, it gets taken down and a new file starts generating. This goes on nonstop. We've been watching it for a few days while trying to get to the FBI, and it just keeps growing and growing."

While the site is being hosted in the United States, Eckelberry said the domain name is registered to an offshore company.

Eckelberry said the huge size of the log files is a clear indication that thousands of machines are pinging back daily.

In some cases, where users appeared to be at immediate risk of losing a considerable amount of money, Sunbelt has contacted the affected individuals.

Eckelberry said the "CoolWebSearch" payload included a typical adware

download that immediately scanned the infected machine for e-mails to use for spam runs. It then sets up a "very intelligent keylogger" that looks for very specific information.

"This won't get caught by a typical anti-spyware application," he said, noting that the keystroke logger was able to pick up identity-related data for delivery to the remote server.

#### Microsoft Receives \$7 Million in Spam Settlement

Microsoft Corp. has won a \$7 million settlement from a man once billed as one of the world's most prolific spammers.

The software maker heralded the deal as a coup in the ongoing fight against unsolicited commercial e-mails, known as spam. Microsoft said the money from Scott Richter and his company, OptInRealBig.com, will be used to boost efforts to combat spam and other computer misuse.

"People engage in spam to make money," Brad Smith, Microsoft's chief counsel, told The Associated Press on Tuesday. "We have now proven that we can take one of the most profitable spammers in the world and separate him from his money. And I think that sends a powerful message to other people who might be tempted to engage in illegal spam."

The deal is the second stemming from joint lawsuits Microsoft and New York state Attorney General Eliot Spitzer filed in December 2003 after Microsoft set "spam traps" that netted some 8,000 messages containing 40,000 fraudulent statements. The lawsuits sought as much as \$20 million in fines against members of a sprawling spam ring.

In the settlement announced Tuesday, Richter and his company agreed to comply with federal and state laws, including CAN-SPAM, the federal Controlling the Assault of Non-Solicited Pornography and Marketing Act. He pledged not to send spam to anyone who has not confirmed a willingness to receive it.

He also agreed to let authorities monitor the business for three years to make sure it does not send any illegal spam.

Attorneys for Richter and OptInRealBig.com, an Internet marketing company based in Westminster, Colo., did not immediately return calls for comment.

In a statement released by Microsoft, Richter said he has changed the way he does business.

"In response to Microsoft's and the New York attorney general's lawsuits, we made significant changes to OptInRealBig.com's e-mailing practices and have paid a heavy price. I am committed to sending e-mail only to those who have requested it and to complying fully with all federal and state anti-spam laws."

Richter was once ranked as the world's third-most prolific spammer. Microsoft said his business sent an estimated 38 million spam messages a year.

Richter and OptInRealBig.com denied allegations they sent misleading e-mails using forged sender names, false subject lines, fake server names

and Internet domain names and addresses registered using pseudonyms and aliases.

However, in a separate settlement announced last month, Richter and OptInRealBig.com agreed to pay New York State \$50,000 in penalties and investigative costs and to use proper identifying information when registering Internet domain names.

Last month, Richter was removed from the Register of Known Spam Operators maintained by the Spamhaus Project, an anti-spam and consumer advocacy group. Since then, Smith said Spamhaus has reported "a massive drop in spam levels."

Stephen Kline, Spitzer's assistant attorney general who handled the case, hailed the settlements as "a step in the right direction." "Will there be others who step in and take some of the business he was doing? Sure," Kline said. "But no one is stepping in that had quite the volume he did."

Tuesday's settlement is conditional on the dismissal of bankruptcy petitions Richter and OptInRealBig.com have pending in U.S. Bankruptcy Court in Denver.

Microsoft has filed more than 135 anti-spam lawsuits worldwide in recent years, about 100 of them in the United States. All told, the company said it has won \$838 million in judgments against spammers.

#### AOL, MSN Seize Spam Assets

America Online and Microsoft are hitting spammers where it hurts most: They are confiscating their assets and giving them away.

AOL, the world's largest Internet service provider, is awarding \$20,000 in gold bars, a 2003 Hummer H2 and \$75,000 in cash it seized from a major spammer as part of a legal settlement last year. It will hold a sweepstakes on its Web site starting Wednesday.

Meanwhile, Microsoft on Tuesday said Scott Richter, once considered one of the world's top spammers, and his company, OptInRealBig.com, agreed to pay \$7 million under a legal settlement. Microsoft is donating \$1 million to a New York program to provide computer gear to community centers. It will spend \$5 million more on anti-spam efforts.

"We think it's justice," says Curtis Lu, AOL deputy general counsel. "We're taking the ill-gotten bounty these spammers have earned off the backs of our customers and handing it back to customers."

The unusual actions illustrate how far AOL and Microsoft are willing to go to discourage spammers, who for years have hounded popular Internet services with unwanted commercial e-mail, and to appease harried users. The largest spammers charge clients up to \$50,000 a month to e-mail ads.

It is the second time AOL has given away assets accumulated by spammers. Last year, AOL awarded a \$45,000 Porsche Boxster.

This year's drawing signifies the effectiveness of the federal Can-Spam Act, Lu says. AOL collected the gold, truck and cash after suing a spammer under the stricter law last year. The lawsuit was one of a dozen AOL filed

since the law went into effect Jan. 1, 2004. It "has struck fear into spammers," Lu says.

The flurry of recent lawsuits has made an appreciable dent in the spam pouring into AOL's and Microsoft's online services, the companies say. Spam is down 85% at AOL, based on member complaints.

Still, spam remains a thorny issue for U.S. consumers and businesses despite high-profile legislation and lawsuits. About 72% of e-mail is spam, up from 68% a year ago, says IronPort Systems, an e-mail security vendor. It says many spammers are shifting targets, from AOL and MSN to businesses and broadband users with less security and fewer legal resources.

Some spammers are adding viruses to steal personal data, computer-security experts say.

"We shouldn't declare victory, but we are turning the tide," says Brad Smith, Microsoft general counsel.

Steve Richter, Scott's father and attorney, said his son has agreed to comply with the federal anti-spam law, and his company is "making every effort to be a model for the best Internet marketing practices."

#### US Officials Go To Hackers' Convention To Recruit

Attention hackers: Uncle Sam wants you.

As scam artists, organized-crime rings and other miscreants find a home on the Internet, top federal officials are trolling hacker conferences to scout talent and talk up the glories of a career on the front lines of the information wars.

"If you want to work on cutting-edge problems, if you want to be part of the truly great issues of our time ... we invite you to work with us," Assistant Secretary of Defense Linton Wells told hackers at a recent conference in Las Vegas.

Wells and other "feds" didn't exactly blend in at Defcon, an annual gathering of computer-security experts and teen-age troublemakers that celebrates the cutting edge of security research.

The buttoned-down world of Washington seems a continent away at Defcon, which was named as a spoof on the Pentagon's code for military readiness derived from "defense condition." Graffiti covers the bathroom walls, DJs spin electronic music by the pool until dawn and hackers who "out" undercover government employees win free T-shirts.

At a "Meet the Feds" panel designed to bridge the cultural divide, a young man waved a pages-long manifesto and demanded, "I would like to know why the federal government, especially some of the law enforcement agencies, are destroying this country."

Despite appearances, hackers and the government have long enjoyed a symbiotic relationship.

Federal research dollars funded development of the Internet and many other cutting-edge technologies, and many hackers first learn the ins and outs



of computer security through military service before moving on to private-sector jobs.

College students in computer-security programs can have their tuition picked up by the government if they agree to work there when they graduate.

The Pentagon is rumored to employ hackers to attack foreign networks. A Pentagon spokesman was not available for comment.

Feds have been a key part of the Defcon audience since its inception in 1992, though they are required to stay at off-site hotels to avoid some of the wilder goings-on.

Along with recruiting, the conference gives federal officials a chance to develop sources and keep up with new research.

"I'm learning while I'm here but I'm also getting the names of people I can maybe call on later so we have a better understanding as cases go along," said Don Blumenthal, who oversees the Internet lab for investigators at the Federal Trade Commission.

Tensions between feds and hackers ran high in 2001 when the FBI arrested Russian programmer Dmitri Skylarov at the conference for writing a program that could break copy protection on electronic books.

The relationship between the two sides has turned less adversarial in recent years, according to long-time attendees, and government employees now account for nearly half of the audience. Some Defcon staffers even hold down day jobs with the National Security Agency and other government shops.

"You can't be deceived by the uniforms," said technology commentator Richard Thieme. "I talked at the Pentagon, and one-third of the people in the audience I already knew from Defcon."

That's not to say that Defcon has gone straight. The ability to break into computer systems is prized above all, and conference attendees whose computers fell prey to their colleagues' attacks are displayed on a "wall of sheep."

Some hackers spent the weekend in their hotel rooms cooking up a new way to take control of the Cisco Systems Inc. routers that underpin much of the Internet.

Many defend this "black hat" approach, arguing that attacks that cause damage in the short term raise awareness of online threats and thus improve the security picture as a whole.

Lynn and other feds made clear that they are not interested in working with those who break into computer systems without permission.

"We're looking for people who haven't crossed that line yet," said Jim Christy, director of the Pentagon's Cyber Crime Institute. "You've got to get folks with the right morals."

The FTC's Blumenthal said that while he was impressed with the honesty of the people he had met, he would double-check the information he receives from them as he does with other sources.

"I have to feel confident that what I'm getting is a straight story," he said. "I find out if I have a curve thrown at me."

## Techies Face Off at Golden Penguin Bowl

Pencil pushers and programmers from Microsoft Corp. and Google Inc. faced off this week for the greatest of geek glories: the Golden Penguin Bowl.

Techies from both companies - rivals in the emerging search engine wars - matched wits Tuesday over questions about everything from old computer operating systems to the name of the mining spacecraft in the movie "Alien."

The quiz competition's announcer dubbed the matchup a battle of "good versus evil," alluding to Google's famous creed of avoiding evil deeds. But officially, this was a battle of Microsoft employees comprising the "Nerd" team against Google's "Geek" squad.

Microsoft's Rob Curran provided a wealth of science fiction knowledge, buzzing in quickly to answer questions about the TV series "Star Trek" and correctly naming the ore mining ship from "Alien" - the Nostromo. Curran took the stage wearing full Darth Vader regalia, while his teammates donned Stormtrooper costumes.

But the Microsoft team bumbled the year their employer released Windows 1.0 (1985).

Google's team correctly answered that the "Debian" Linux distribution was named after Ian Murdock and his then-girlfriend Debra.

Buzzers went silent, though, after a question about science reality. What was NASA's name for the mission designed to explore the comet Tempel 1? (Correct answer: Deep Impact.)

For the record, Google won the contest.

The event took place at the LinuxWorld Conference & Expo, which focuses on the Linux operating system and open source software solutions.

## Get Ready for Firefox 1.5

The next version of the popular Firefox Web browser has undergone a name change to 1.5 and will be released for beta testing in September. The Mozilla Foundation plans to release the full version by the end of this year.

Some analysts credit the growing popularity of the Firefox browser with Microsoft's move to speed up the deployment of its long-overdue upgrade of Internet Explorer. Industry experts say Firefox has siphoned off about 10 percent of Internet Explorer's market share.

Various posts on Mozilla's Web site report that the decision to jump to version 1.5 from the current version of Firefox, now at 1.0.6, resulted from an unrealistic time frame associated with shipping the next update, originally planned for August.

According to Mozilla Europe President Tristan Nitot, the next major version of Firefox will contain more new features than the organization originally estimated. "What we have been doing is better than initially planned, so instead of calling it 1.1, we think it deserves the name of 1.5," he wrote.

Nitot said the organization has tweaked Firefox's core programming over the past 16 months. Simply issuing a version update named Firefox 1.1 would be misleading to product users, he explained.

The new features planned for Firefox 1.5 include better overall functionality and an improved extensions system. Firefox uses extensions - free add-on programs contributed by third-parties - to add customized features to the Web browser.

A major new feature in Firefox 1.5 is support for Scalable Vector Graphics (SVG), a specification for rendering two-dimensional graphics in browser interfaces. SVG works much like Macromedia's proprietary Flash technology but is an open standard.

Much of the popularity of Firefox has been because of consumers. Businesses have been slow to adopt the alternative browser because of worries about compatibility issues.

"Firefox is not making a big impact yet in the corporate world," said Nate L. Root, vice president and research director of customer service for Forrester Research. But Root noted that recent moves by Mozilla developers to form a for-profit corporation will bring Firefox one step closer to being something CIOs can consider.

"Right now it is largely viewed as an experimental product - and rightly so - and is not yet ready for prime time," said Root.

#### Yahoo Buys Into Chinese Online Company

Yahoo Inc. is paying \$1 billion in cash for a 40 percent stake in China's biggest online commerce firm, Alibaba.com, strengthening the ties that international companies are forging in the world's second-largest Internet market.

Yahoo said it will merge its China subsidiaries into Alibaba as part of Thursday's deal, the biggest in a flurry of investments by foreign Internet firms eager for access to China's soaring number of Web users, now pegged at 100 million.

"This is Yahoo getting much bigger in China," Daniel Rosensweig, Yahoo's chief operating officer, said at a news conference in Beijing with Alibaba founder Jack Ma.

Alibaba runs a Web site that matches foreign buyers with Chinese wholesale suppliers, plus the popular consumer auction site Taobao.com, which competes with the Chinese subsidiary run by eBay Inc., the world's top online auction company.

Rosensweig said the alliance creates an entity with assets to compete across the full range of Internet businesses - online commerce, e-mail and search engines. He expects China to become the world's biggest Internet market within five years.

The deal extends Sunnyvale, Calif.-based Yahoo's strategy of breaking into Asian markets by connecting with strong local partners. Yahoo and its Asian partners are now major forces in online auctions in China, Japan, Taiwan and Hong Kong, said Porter Erisman, Alibaba's vice president for international relations.

"This is really probably the knockout blow for eBay in China," he said.  
"This is going to make it hard for eBay to win in Asia."

EBay, which bought the Chinese auction portal Eachnet for \$180 million in 2003, rejected suggestions that the Yahoo-Alibaba tie-up was a threat. EBay's share of China's auction market is 65 percent, according to Shanghai iResearch. TaoBao had 29 percent in 2004.

"It's business as usual for us," said eBay spokesman Hani Durzy in San Jose, Calif.

That sounded like careful posturing to Hoefer and Arnett analyst Martin Pyykkonen. He noted that eBay CEO Meg Whitman has predicted that China will become the company's biggest market in five years, so the Yahoo-Alibaba alliance signifies "more than just a casual threat," he said.

China is expected to be a significant profit center for eBay this year or next, but eBay needs to start capitalizing on its investments in the country in 2007 and 2008 to propel earnings growth, he said. EBay is expected to invest about \$100 million in China this year, Pyykkonen estimated.

The new Yahoo-Alibaba combination will include 3721.com, a Chinese-language search engine that Yahoo acquired last year for \$120 million.

That will put it in competition with China's most popular search engine, Baidu.com, whose initial stock offering in the United States last week set off a buying frenzy. Its share price soared more than 350 percent in its first day of trading before declining this week.

And the second-most popular Chinese search site is operated by a familiar rival, Google Inc. Google ramped up its China operations this week by authorizing three Chinese companies as resellers of advertisements for its China site. Google also owns 2.6 percent of Baidu.

The Chinese government says the country has 103 million people online, second only to the United States. But online commerce is still small, held back by low consumer spending in a country where urban incomes average just \$1,000 a year.

Consumer-to-consumer online auctions in China totaled about \$500 million last year, while business-to-consumer sales were about \$1 billion, according to Joe Tsai, Alibaba's chief financial officer. He said only about 4 million people in China have used online commerce.

But Tsai said online sales are expected to grow 80 percent annually over the next three years.

With its 40 percent stake valued at \$1 billion, Yahoo clearly expects huge growth from Alibaba, whose revenue was \$68 million last year. Advertisers and companies pay \$5,000 to \$10,000 per year for membership in its commercial online auction service. It does not charge fees for individual auction listings as eBay does.

Yahoo said its investment will make it the biggest shareholder in Alibaba, which has 2,300 employees and is based in the eastern Chinese city of Hangzhou, southwest of Shanghai.

Yahoo will have 35 percent voting rights. The new entity will have a four-member board led by Ma as chairman, with a second seat held by Alibaba and the others held by Yahoo co-founder Jerry Yang and a representative of Softbank Corp., the Japanese firm that is a big Yahoo shareholder.

Pykkonen called that a departure for Yahoo and CEO Terry Semel, because the company usually takes control of a partner's operations when it spends this kind of money. The arrangement could lead to some friction, he predicted.

"Ma has a reputation for being a bit of a cowboy," Pykkonen said. "Terry Semel won't be able to rein him in as easily."

Alfred Tolle, head of Internet rival Lycos Inc., which recently opened an office in Shanghai and launched a social networking site in China, said he believes Yahoo overpaid for a 40 percent stake.

Tolle said he isn't interested in making an acquisition in the country, and added that the recent fascination with Chinese Internet companies reminds him of the dot-com boom in the United States a few years ago.

"It's getting a little overheated in China," he said, "a bit like 1999 or 2000."

#### GPL Upgrade Due in 2007

The planned upgrade to the GNU General Public License (GPL) will be ready by 2007, according to an industry official involved with the project.

Presenting at the LinuxWorld conference on Wednesday, Eben Moglen, president and executive director of the Software Freedom Law Center and a key participant in the planned Version 3.0 of GPL, cited issues expected to be covered in the upgrade. These include resolving patent conflicts, accommodating Web services, and resolving incompatibilities with other licenses. Dealing with wikis in the GPL also has been pondered.

The Free Software Foundation, which has jurisdiction over the GPL, seeks compatibility with the Apache Software license, said Moglen, who serves on the foundation's board of directors.

"We will take some steps to increase the compatibility of the GPL with some non-GPL licenses whenever possible, without adversely affecting freedom," Moglen said. Lately, companies such as Sun Microsystems, with its Common Development and Distribution License (CDDL), have developed their own brands of open source licenses.

Moglen did not mince words when speaking on what the foundation thinks about patents. "Its position is that the application of patent law to software is dangerous and unproductive," he said. "All we're saying is the disastrous, 15-year American experiment with patenting software ought to be terminated."

Patent conflicts have clouded open source development, with developers and others fearing that the open source code they distribute may unknowingly be subject to someone else's patent and attendant royalties. "Everybody understands the patent problem is deeply serious," Moglen said.

Version 3.0 is not about fixing or repairing the GPL but bringing it up to date after a long life for GPL 2, he added. "We have been using GPL 2 for quite a while and 15 years is probably long enough. It's about time for a change."

However, he also stressed, "we will do nothing [to change the GPL] that we have not studied exhaustively."

Foundation president Richard Stallman will ultimately make judgments on what transpires with the new GPL, Moglen said.A

A draft of GPL 3.0 is expected in late-2005 or early-2006, followed by a full calendar year of discussions, revisions, and other input, Moglen said.

The move to the new GPL will likely take place in the first few days of 2007. Some 150,000 individuals around the world are expected to comment, with Version 3.0 expected to be the largest, non-governmental act of legislation in the history of the world.

A global conference on translation of the GPL is likely to be held in Europe, with possibly a follow-up event to occur in Asia. The upgrade of the GPL will be international and involve advisory committees.

Moglen expects deliberations to be civil, with no flame wars likely. He also anticipates that users will quickly migrate to Version 3.0. "When this process is over, I think the number of Version 2 holdouts is going to be infinitesimal," he said.

Changes are also likely with the GPL sister license, the GNU LGPL (Lesser GPL).

Also at LinuxWorld on Wednesday, IBM Senior Vice President Steve Mills stressed the desktop as the next frontier for Linux. Having had vast success in server environments, the Linux client environment is "the next frontier," Mills said.

Canada-based Pioneer Petroleums has been leveraging Linux on the client, using Linux from Red Hat and IBM's Workplace messaging software, according to IBM. The Linux desktop market will have a compound annual growth rate of 37 percent from 2003 to 2007, based on research that Mills presented.

#### Nearly A Third Of Online Americans Have Visited Blogs

The number of people in the United States who visited web logs in the first quarter of the year reached 50 million, and each of the top four hosting services for blogs on the Internet topped 5 million visitors, a web metrics firm said Monday.

The number of Americans visiting blogs amounted to 30 percent of the total online U.S. population, an increase of 45 percent over the same period last year, ComScore Networks said.

Other key findings in the report were that the top four hosting services for blogs had more than 5 million unique visitors. Those sites in order, starting with the largest, were Blogspot.com, Livejournal.com, Typepad.com and Xanga.com.

Blogspot.com's 19 million unique visitors amounted to more visitors than the NYTimes.com, USAToday.com and WashingtonPost.com. The numbers were "clear evidence that consumer-generated media can draw audience on par with traditional online publishers," the report said.

Five individual blogs had more than a million unique visitors. In order, starting with the largest, were FreeRepublic.com, DrudgeReport.com, Fleshbot.com, Gawker.com and Fark.com.

In general, political blogs were the most popular, followed by "hipster" lifestyle blogs, tech blogs and blogs authored by women.

Compared to the average Internet user, blog readers tended to be significantly more likely to live in wealthier households, be younger and connect to the web on high-speed connections. Blog readers also visited nearly twice as many web pages as the average Internet user, and were much more likely to shop online.

"The fact that we found 30 percent of the online population to have visited blogs clearly underscores the commercial importance of consumer generated and driven media," Dan Hess, senior vice president of ComScore, said in a statement. "It's noteworthy that while the blog audience is already quite large and growing, its demographic composition relative to the total population will appeal to many marketers."

The study was sponsored in part by blog-hosting service Six Apart and by Gawker Media.

=~::~~::~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: [dpj@atarinews.org](mailto:dpj@atarinews.org)

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.